



Date de réception : 23/01/2015

WRITTEN OBSERVATIONS OF THE REPUBLIC OF SLOVENIA

Case C-362/14*

Document lodged by:

The Republic of Slovenia

Usual name of the case:

SCHREMS

Date lodged:

5 November 2014 (eCuria)

Court of Justice of the European Union

Case C-362/14

Schrems

Written observations of the Republic of Slovenia

[Or. 2]

1. Introduction

- 1 In accordance with the second paragraph of Article 23 of the protocol on the Statute of the Court of Justice, the Republic of Slovenia presents its written observations on the reference for a preliminary ruling from the Court of Justice of the European Union ('the Court') made by the High Court of Ireland ('the referring court') in the proceedings pending before it, Schrems v Data Protection Commissioner, under Article 267 TFEU.

2. The facts and background to the case

- 2 The referring court presents in its order for reference the factual and legal context of the case; Slovenia refers to that entirely, in order to avoid repetition.

* Language of the case: English.

- 3 The High Court of Ireland states in its order that the validity of the administrative decision of the Data Protection Commissioner not to carry out an examination of Mr Schrems' complaint depends on the correct interpretation and application of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹ ('the 1995 Directive') and Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the 'safe harbour' privacy principles and related frequently asked questions issued by the US Department of Commerce² ('the Safe Harbour Decision').
- 4 The referring court notes, in addition, that the applicant in the main proceedings in reality makes a 'complaint concerning the terms of [the Safe Harbour Decision] rather than the manner in which the Commissioner had applied it'. The applicant does not contest the validity of the 1995 Directive or the validity of the Safe Harbour Decision (paragraphs 18, 20 and 25 of the order for reference), nor raise any issue as to the actions of the companies Facebook **[Or. 3]** Ireland Ltd or Facebook Inc. (paragraph 19 of the order for reference). On that basis, the referring court took the view that in reality, in the case at issue, the question was whether the Data Protection Commissioner was bound by the Safe Harbour Decision under which the US guaranteed a level of protection of personal data consistent with Article 25(6) of the 1995 Directive, and this question arose, in particular, in view of the revelations made by Mr Snowden as regards the activities of the US National Security Agency ('NSA') and the gaps in US practice and legislation as regards personal data and the subsequent entry into force of the Charter of Fundamental Rights in the European Union ('the Charter').
- 5 The referring court states at paragraph 19 of the order for reference that Article 3(1)(b) of the Safe Harbour Decision allows a national authority to direct any organisation to suspend data flows to the third country in question. The court considers, however, that that is not possible unless the complaint is directed to the conduct of that organisation. In the present case, on the contrary 'the real objection is not to the conduct of Facebook as such, but rather to the fact that the Commission has already determined that the US law and practice provides adequate data protection in circumstances where it is clear from the Snowden disclosures that personal data of EU citizens so transferred to the US can be accessed by the US authorities on a mass and undifferentiated basis' (paragraph 19 of the order for reference).
- 6 In those circumstances, the referring court referred to the Court of Justice the following questions:

¹ – OJ 1995 L 281, p.31

² – OJ 2000 L 215, p. 7.

‘Whether in the course of determining a complaint, which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 474 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding?’

Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?’

3. Law

3.1 Legal Framework: TFEU, the Charter and the European Convention on Human Rights

- 7 The protection of personal data occupies a very high level in the European Union agenda. Article 16 TFEU, which is within Title II ‘Provisions having general application’, provides that ‘Everyone has the right to protection of personal data concerning them.’ It also requires the Union legislature to adopt an appropriate legislative framework in that field.
- 8 Article 8 of the Charter recognises the right to the protection of personal data as an autonomous³ right governed by a specific article, distinct from the right to respect for private and family life. That right is nevertheless closely linked to the right to private life under Article 7 of the Charter.⁴ It is in fact a specific expression of the protection of private life (see, for example, judgments of 29 January 2008, *Promusicae*, C-275/06, ECR p. I-271, paragraphs 63 and 64 and of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, ECR p. I-11063, paragraph 47). In a manner similar to the right to private life, which is an expression of human dignity and personal liberty, the right to protection of personal data has its roots in the idea that a democratic society is not to be based on control, profiling, classification or discrimination.⁵

³ – Ferretti F. ‘Data protection and the Legitimate Interests of Data Controllers: Much Ado about Nothing or the Winter of Rights’ 51 CMLR (2014) 843-868, p. 843 and 853.

⁴ – As regards the protection of personal data, see also Kokott and Sobotta ‘The Distinction between Privacy and Data Protection in the jurisprudence of the ECJ and the ECtHR’ 3 International Data Privacy law (2013) 222 – 228.

⁵ – Ferretti F. ‘Data protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights’ 51 CMLR (2014) 843-868, p. 849.

- 9 The right to protection of personal data is not an absolute right; it must, on the contrary, be considered having regard to the role that it has in society (see judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, Rec. p. I-11063, paragraphs 47 and 48). Article 8(2) of the Charter thus allows the processing of personal data if certain conditions are fulfilled. According to that provision, ‘such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.’ Under Article 52(1) of the Charter, the exercise of the rights and freedoms, such as Articles 7 and 8 of the Charter, may be limited if the limitation is provided for by law, respects the essence of those rights and freedoms and if – having regard to the principle of proportionality – they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (see the judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 38).
- 10 It should also be noted in that context that, in accordance with Article 52(3) of the Charter, the meaning and scope of the rights which correspond to the rights guaranteed by the Convention on the Protection of Human Rights and Fundamental Freedoms (‘ECHR’) is the same as the meaning and scope of the rights laid down by that convention. As the Court stated in Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* (at paragraph 52 of the judgment), the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 ECHR. Under Article 8 ECHR, everyone has the right to respect for his or her private and family life, home and correspondence. ‘There is to be no interference by a public authority with the exercise of that right, except *such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*’ (emphasis added).
- 11 According to the settled case-law of the European Court of Human Rights, the interference with the rights under Article 8 ECHR must be, inter alia, ‘in accordance with the law’, but that phrase not only concerns national legislation in itself, but also relates to the quality of the legislation and the requirement to comply with the rule of law. That phrase means, therefore – as is apparent from the subject matter and purpose of Article 8 – that measures of national law which guarantee legal protection from interference by public authorities with the rights guaranteed are binding. The risk of arbitrary action is all the more apparent when a public authority acts in secret (see case *Klass and Others v Germany*, of 6 September 1978, Application No 5029/71). [Or. 6] ‘*The requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place*

*restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, **the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.***’ (our emphasis) (Case *Malone v United Kingdom*, 2 August 1984, Application No 8691/79, paragraph 67).

- 12 In the case *Liberty and Others v United Kingdom*, the European Court of Human Rights again stated the importance of foreseeability of the interference in the right to private life by secret surveillance measures. That court set out the minimum guarantees that the law must contain in order to prevent the arbitrary use of public power: (1) the nature of the offences which may give rise to an interception order; (2) the categories of people and (3) the duration of the interception of communications; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties and (6) the circumstances in which recordings may or must be erased or the tapes destroyed (see the judgment of 1 July 2008, Application No 58243/00, paragraph 62).
- 13 The fight against international terrorism with the aim of maintaining international peace and security is, according to the case-law of the court, an objective of general interest to the European Union (see the judgment in *Kadi and Al Barakaat International Foundation v Council and Commission*, C-402/05 P and C-415/05 P, EU:C:2008:461, paragraph 363). The same is true of the fight against serious crime in order to ensure public security (see the judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 42 and the judgment of the Court of Human Rights in *Kennedy v The United Kingdom* of 18 May 2010, Application No 26839/05, paragraph 155). It is necessary also, however, to ensure, in any event, that the limitation of the rights under Article 7 and 8 of the Charter is proportionate with respect to the legitimate objective it implements (see, in particular, the judgment of the European Court of Human Rights in the case *Gillow v The United Kingdom* of 24 November 1986, series A No 109, paragraph 55 and [Or. 7] the judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, ECR. p. I-4989, paragraph 83 and *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 46 and following).
- 14 The cited legal framework for the protection of personal data constitutes, according to the Republic of Slovenia, the ‘minimum requirement’ to guarantee that any interference with the individual’s fundamental right to private life is foreseeable, legitimate and does not go further than is necessary in a democratic society. Having regard to the nature of the Charter, which by virtue of Article 6

TEU has the same value as the Treaty, it is necessary, according to Slovenia, to interpret all EU acts (in this case, the 1995 Directive and the Safe Harbour Decision) in accordance with the Charter and the meaning that the case-law of the Court gives to it. Thus, in accordance with Article 51(1) of the Charter, the Member States must apply its provisions when they implement European Union law (judgment of 21 December 2011, *N.S. and Others*, C-411/10 and C-493/10, not yet published, paragraphs 64 to 69).

3.2 *The Safe Harbour Decision*

- 15 In 2000, the European Commission ('the Commission') found in the Safe Harbour Decision, under Article 25(6) of the 1995 Directive, that the United States guaranteed a sufficient level of protection for data. That finding applies to organisations that have committed themselves to adhering to the Safe Harbour principles, which amounts to an assurance that its organisations adequately protect personal data. It is therefore a code of conduct on the basis of which the Commission found that an adequate level of protection of personal data originating in the Member States of the EU and transferred to organisations in the United States was guaranteed, even though the transfer of data, having regard to the known differences in the legislation on the protection of private life in the EU and the United States, would not satisfy EU standards in terms of an adequate level of protection of data.⁶
- 16 The Safe Harbour regulatory regime in force rests on organisations' voluntary agreements and their self-certification with the US Department of Commerce; the organisations agree to adhere to the Safe Harbour principles and make a public declaration of that in their data protection policies. The compliance with their undertakings rests on the legal mandate of the competent authorities in the US, which are empowered to examine complaints in cases of unfair practices. **[Or. 8]** In accordance with the Safe Harbour principles, the organisation must inform individuals as to *the purposes* for the collection and use of their data. The organisation must offer the individual the choice whether his personal data will be divulged to third parties or whether they are used for a purpose other than that for which they were collected. The adherence to the Safe Harbour principles may, in accordance with Annexe I of the Safe Harbour Decision, be limited, 'to the extent necessary' to meet national security, public interest or the respect of US law, and by statute, government regulation or case-law. In accordance with the objective of enhancing privacy protection, organisations should strive to implement the principles fully and transparently, including indicating in their privacy policies when permitted exceptions will apply.⁷

⁶ – See the Report of the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 Final of 27 November 2013, paragraph 1, p. 2.

⁷ – Annex 1 to the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of the protection provided by the

- 17 As the referring court states in its order for reference: ‘there is [...] much to be said for the argument that the Safe Harbour Regime has been overtaken by events’. In spite of the commitments made, the Snowden revelations have exposed substantial lacunae in contemporary US practice and legislation regarding the protection of personal data. As the Commission also states in its Communication to the European Parliament and Council ‘*While the exceptional processing of data for the purposes of national security, public interest or law enforcement is provided under the Safe Harbour scheme, **the large scale access by intelligence agencies to data transferred to the US in the context of commercial transactions was not foreseeable at the time of adopting the Safe Harbour***’ (our emphasis).⁸ ‘*As results from the findings of the ad hoc EU-US Working Group*⁹ on data protection, a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed by companies based in the US. ... [Or. 9] *The large scale nature of these programmes may result in data transferred under Safe Harbour being accessed and **further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in the Safe Harbour Decision***’ (our emphasis).¹⁰ The Commission states in the same communication that ‘**companies do not systematically indicate in their privacy policies when they apply exceptions to the Principles**. The individuals and companies are thus not aware of what is being done with their data. This is particularly relevant in relation with the operation of the US surveillance programmes in question. As a result, Europeans whose data are transferred to a company in the US under Safe Harbour may not be made aware by those companies that their data may be subject to access’ (emphasis added).¹¹
- 18 Slovenia considers, on the basis of the findings of the ad-hoc EU-US Working group on Data Protection and the Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, that it may be concluded with a high degree of probability that some organisations do not consistently put into effect the commitments made and that the work of the US

safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

⁸ – See Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU. COM(2013) 847 Final of 27 November 2013, paragraph 7, p. 19.

⁹ – See the Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection of 27 November 2013.

¹⁰ – See Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU. COM(2013) 847 Final of 27 November 2013, paragraph 7.1, p. 20.

¹¹ – See the Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU. COM(2013) 847 Final of 27 November 2013, paragraph 7.3, p. 20

authorities is not transparent,¹² which constitutes a disproportionate and legally unforeseeable interference in the right to protection of personal data (see, in particular, paragraphs 9 to 13 of the written observations).

3.3 Obligation to take account of the Commission findings contained in the Safe Harbour Decision

- 19 According to Slovenia's understanding of the questions asked by the referring court in its order for reference, that court wonders, in essence, whether it is bound by the Commission's findings set out in the Safe Harbour Decision, according to which US legislation and practice guarantee adequate protection for [personal] data, or whether it may, or even must, conduct its own investigation of the matter in the light of factual developments since the Commission's decision was first published. The dilemma facing the High Court of Ireland results from the fact that the applicant in the main proceedings does not challenge either the legality of the 1995 Directive or that of the Commission's Safe Harbour Decision and, likewise, does not raise any issue regarding the actions of the companies Facebook Ireland Ltd or Ireland Inc., but in fact contests the provisions of the Safe Harbour regime itself **[Or. 10]** (see paragraphs 4 and 5 of the written observations). It is not possible therefore, according to the referring court, to apply Article 3(1)(c) of the Safe Harbour Decision. Slovenia cannot subscribe to the position taken by the referring court; Slovenia considers that Article 3(1)(b) of the Safe Harbour Decision is the correct legal base upon which the national authority must act in the appropriate manner in the event of infringement,¹³ that is to say, order the suspension of transfer of personal data on the basis of the provisional examination.
- 20 As Slovenia has already stated in paragraph 14 of these observations, it is necessary, having regard to the hierarchy of norms, to interpret all EU acts (in this case, the 1995 Directive, and the Commission's Safe Harbour Decision) in accordance with the Charter and the interpretation given to it by the Court of Justice. Slovenia is of the view that taking account of the Commission's findings in the Safe Harbour Decision to the effect that the US legislation and practice guarantee adequate protection of personal data, despite the contrary findings that were made later, manifestly goes against the hierarchy of norms in the EU's legal system. That approach would mean that the Commission's finding constitutes an irrebuttable legal presumption (*praesumptio iuris et de iure*) and therefore a presumption against which it would not be possible to adduce evidence. Article

¹² – See the summary of the main findings, of the Report on the findings by the EU Co-chairs of the ad-hoc EU-US Working group on Data Protection of 27 November 2013 : large-scale access by intelligence agencies to data transferred to the US; differences in legal protection on the basis of whether the subjects are from the EU or the US and as to the type of personal data; lack of clarity as to the legal bases of surveillance; lack of administrative/judicial protection, etc.

¹³ – Article 3(1) of the decision uses, it is true, the term 'may'; however, that term must, according to Slovenia, be interpreted as being imperative, 'must'.

3(1)(b) of the Safe Harbour Decision, however, expresses the opposite, namely, that the decision itself provides guarantees in the event of breach.

- 21 Slovenia considers, in addition, that applying Article 3(1)(b) of the Safe Harbour Decision specifically allows an outcome consistent with the Charter to be achieved. Article 3(1)(b) must be interpreted broadly as regards the national authorities' options for examining the case¹⁴ given the particular nature of the Safe Harbour Decision, for it establishes a regulatory regime that departs from the ordinary regulatory framework applicable to the transfer of data to third countries.
- 22 As Article 3(1)(b) of the Safe Harbour Decision makes clear, that provision may not be applied unless the following conditions are satisfied:
 - (1) there is a substantial likelihood that the principles are being violated; **[Or. 11]**
 - (2) there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue;
 - (3) the continuing transfer would create an imminent risk of grave harm to data subjects; and
 - (4) the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

(1) As regards the substantial likelihood that the principles are being violated

- 23 It would indeed be possible to conclude purely on the basis of a literal interpretation of Article 3(1)(b) of the Safe Harbour Decision that that provision does not allow the competent national authority to intervene except in the event of (probable) breaches committed by organisations (therefore companies) in the US, but does not allow the authority to act in the event of breaches arising out of a lack of transparency or implementation of the Safe Harbour principles on the part of the US authorities. According to Slovenia, it is, however, very difficult in the present case to distinguish between the actions of organisations (Facebook) that fall with the Safe Harbour regime, and the methods applied by the US authorities. The findings of the ad-hoc EU-US Working group on Data Protection show, on the one hand, that the US authorities may access data transferred under the Safe Harbour regime and subsequently process that data to an extent greater than is strictly necessary for, and proportionate to, the protection of national security. On the other hand, the companies themselves also, in their privacy policies, do not

¹⁴ The Slovenian competent authority has not, so far, adopted measures on the basis of the article at issue, nor does Slovenia have information on the use of that provision in other Member States, and it therefore concludes that the provision has been narrowly interpreted until now.

systematically indicate when they apply the exceptions to the Safe Harbour principles. It is, in this respect, apparent from the summary of the main findings of the ad-hoc EU-US Working group on Data Protection that the companies are required to keep secret the fact that they are obliged, under an order of the Foreign Intelligence Surveillance Court, to transfer personal data, including that of EU citizens, to the US authorities.¹⁵ Failure to observe the Safe Harbour principles is therefore complex and involves aspects closely linked to one another. According to Slovenia, it is not conclusive for the ruling in the present case whether the companies actively collaborated with the US authorities and whether they knew of the secret surveillance operations.¹⁶ The close relationship between the conduct of the self-certified organisations [Or. 12] and the conduct of the public authorities could, therefore, according to Slovenia, reduce to no purpose the effectiveness of Article 3(1)(b) of the Safe Harbour decision. The provision at issue must therefore be interpreted in the light of the purpose pursued by the Safe Harbour regime, namely, to ensure the protection of personal data in accordance with the Charter and the ECHR. The Safe Harbour Decision must be interpreted dynamically, by attaching to time and technological development that which is all the more important in the field of protection of personal data.

- 24 There are differences between the Member States of the European Union and the United States as regards the interpretation and application of the exception on grounds of 'national security'. National security is indeed, according to the TEU, within the competence of the Member States; that does not, however, exclude the application of the Charter to interference in private life by national authorities acting on the basis of that exception. Every exception must be strictly interpreted. Slovenia is of the opinion that the only guarantee that there will not be too wide an interpretation of that exception is the coherent application of the principle of proportionality, which is also contained in the Safe Harbour Decision. The rule, and the exception to the rule, must therefore be assessed together. For that reason, in this case, it is not possible to make a clear distinction between conduct on the part of the organisation (Facebook) that falls within the Safe Harbour regime and the conduct of the US authorities.
- 25 As Slovenia has already stated at paragraph 23 of these observations, referring to the findings of the ad hoc EU-US Working Group on Data Protection, the US authorities access data transferred under the Safe Harbour regime and process it to an extent greater than is strictly necessary and proportionate for national security. The proportionality test has not, therefore, in the present case, been satisfied, for the NSA has collected data on an indiscriminate, large-scale basis (that is to say that the NSA amassed too broad a collection of data for an objective that was too

¹⁵ – See the Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection of 27 November 2013.

¹⁶ – As the case of Yahoo shows, NSA required the organisation to cooperate with it, but at the same time, the organisations had a degree of room for manoeuvre in that cooperation. See: http://www.nytimes.com/2014/09/12/technology/documents-unsealed-in-yahoos-case-against-us-data-requests.html?_r=2

broadly defined (not targeted)) and that it has, therefore, breached legal standards as recently defined by the Court in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd.* Slovenia notes at this point that the criteria of necessity and proportionality also follow from the EU's position in the negotiation of the Safe Harbour: ¹⁷ **[Or. 13]**

'It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.'

- 26 As the Commission stated in its Communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, 'any lack of transparency and any shortcomings in enforcement undermine the foundations on which the Safe Harbour scheme is constructed'.¹⁸ Slovenia considers therefore that the independent official, whose function, under the law, is to implement the data protection legislation, must (and not merely may), in the circumstances of the present case carry out his own examination of the case having regard to the actual development of events since the initial publication of the Commission's decision and adopt appropriate decisions on the basis of Article 3(1)(b) of the Safe Harbour Decision. The Commission's task is, on the basis of Article 25 of the 1995 Directive, to commence or continue the dialogue with the US as regards the guarantee of adequate protection of personal data and to adopt, if necessary, an appropriate decision under Article 25(4) or (5) of the directive.

(2) Whether there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue

- 27 In the light of the limited information available, Slovenia considers that this condition is satisfied. As is apparent from the Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, the US legal system does not contain an adequate mechanism for protecting individuals' rights.¹⁹ Slovenia notes that the negotiations between the Commission and the United States on the Safe Harbour are continuing, while the ad hoc EU-US Working Group on Data Protection, which was concerned with setting out the factual situation, delivered its report only in November 2013. **[Or. 14]**

¹⁷ – http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf [Paragraph 13] [Ndt: le texte n'existe qu'en version anglaise]

¹⁸ – See the Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU. COM(2013) 847 Final of 27 November 2013, paragraph 2.2, p. 5.

¹⁹ – Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection of 27 novembre 2013, paragraph 4.3.

(3) *Whether the continuing transfer would create an imminent risk of grave harm to data subjects*

- 28 In the present case, perhaps the most difficult question is whether the continuing transfer of data would create for Mr Schrems a risk of grave harm within the meaning of Article 3(1)(b) of the Safe Harbour Decision. Given the secret nature of NSA operations, it is very difficult, even impossible, to obtain direct proof that the NSA has also processed Mr Schrem's personal data. Slovenia indicates, in that regard, that according to the settled case-law of the European Court of Human Rights, in order to conclude that there has been interference with an individual's private life, it suffices that 'there was a reasonable likelihood that surveillance measures were applied to the [person concerned]' (see the judgment of the European Court of Human Rights in the case *Kennedy v The United Kingdom*, of 18 May 2010, Application No 26839/05, paragraphs 123 and following; the earlier case *Klass and Others v Germany*, of 6 September 1978, Application No 5029/71).²⁰ A requirement to produce concrete proof that the secret surveillance measures interfered with the private life of the individual would deprive Article 3(1)(b) of the decision of all practical value. Slovenia therefore considers that in the present case the condition that 'the continuing transfer would create an imminent risk of grave harm to data subjects' is satisfied.
- 29 Slovenia submits that the breach of fundamental rights (in this case, the right to private life) undoubtedly involves grave harm for the persons concerned. It follows from Article [25](6) of the 1995 Directive, which is the legal basis for the adoption of the Safe Harbour Decision, that 'the Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, **for the protection of the private lives and basic freedoms and rights of individuals**' (emphasis added). Thus, respect for fundamental rights is a fundamental element of the 'adequate level' of protection of personal data in third countries. [Or. 15]
- 30 In order to establish the existence of interference with the right to private life, it does not matter, according to the case-law, whether the personal data at issue is of a sensitive character or whether the persons concerned have suffered any damage (see to that effect the judgments in *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 75 and *Digital*

²⁰ – See also to that effect 'Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' of 23 September 2014, p. 19. The report concentrates on the use of mass digital surveillance with the aim of fighting terrorism and its interaction with Article 17 of the International Covenant on Civil and Political Rights <http://justsecurity.org/wp-content/uploads/2014/10/EmmersonReportMassSurveillance.pdf>. The Report is also in view of its wider international dimension.

Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33). Any act that involves a disproportionate interference with the fundamental right to private life constitutes non-material damage for the person concerned.

- 31 Since the Safe Harbour Decision provides an exception to the Safe Harbour principles in respect of, inter alia, national security, Slovenia is of the opinion that *a fortiori* there must be, for this type of processing of personal data, a competent authority in the US which enables the independent assessment of the legality of interference in private life. In the light of those considerations, the national competent authorities of the Member States under Article 3(1)(b) of the Safe Harbour Decision are all the more important because they ensure a minimum supervision of the implementation of the Safe Harbour principles and the protection of personal data. In accordance with the Court's case-law, the control by an independent authority, as required by Article 8(3) of the Charter, of the protection of personal data is a fundamental component of the protection of that data (see the judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 68). Slovenia notes in this context that the Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, clearly showed that the US legal system contains no adequate mechanism for the protection of the rights of individuals.²¹ Thus, the legal protection required by Article 47 of the Charter is not ensured.

Whether the competent authorities in the Member State have made reasonable efforts in the circumstances to provide the organisation with notice and an opportunity of responding

- 32 The order for reference does not make it clear whether the national competent authority made efforts to inform the organisation of the facts of the case at issue or whether it gave that organisation the opportunity of responding as regards the breaches alleged. In this regard, Slovenia is of the opinion **[Or. 16]** that the competent national authority must invite the company in question to give its observations on the breaches alleged. The competent authority must also inform the Commission and the other Member States immediately of the likely breaches, as required by Article 25(3) of the 1995 Directive. Only in that way is it possible to ensure a uniform approach by the Member States and the EU institutions regarding the protection of personal data. **[Or. 17]**

Conclusion

Having regard to the factual and legal context of the questions referred, Slovenia suggests that the Court should reply as follows:

²¹ – Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection of 27 November 2013, paragraph 4.3.

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce must be interpreted in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (2000/C 364/01).

The independent officer, whose function under the law is to implement the legislation on the protection of personal data and who applies that law must, in his decision on a complaint alleging that personal data was transferred to a third country (in this case, the United States of America) in which the law and practice allegedly does not provide adequate protection for the persons concerned, carry out, on the basis of Article 3(1)(b) of the Safe Harbour Decision, his own examination of the case taking into account factual developments and events since the initial publication of the Commission's decision if the four conditions under Article 3(1)(b) of the decision are satisfied. The independent officer has, under the options entrusted to him under Article 3(1)(b), the power to order an organisation that exports data to cease transferring that data.

For the Republic of Slovenia

[Signature]